



WLM-1500/2500/3500



Wireless ADSL2+ Modem Router

# User Manual

Version: 1.0

## TABLE OF CONTENTS

---

<b>1</b>	<b>KEY FEATURES .....</b>	<b>4</b>
<b>2</b>	<b>PACKAGE CONTENTS .....</b>	<b>5</b>
<b>3</b>	<b>PRODUCT LAYOUT .....</b>	<b>6</b>
<b>4</b>	<b>SYSTEM REQUIREMENTS.....</b>	<b>8</b>
<b>5</b>	<b>WLM-1500/2500/3500 PLACEMENT .....</b>	<b>8</b>
<b>6</b>	<b>SETUP LAN, WAN .....</b>	<b>9</b>
<b>7</b>	<b>PC NETWORK ADAPTER SETUP.....</b>	<b>10</b>
<b>8</b>	<b>BRING UP THE WLM-1500/2500/3500.....</b>	<b>13</b>
<b>9</b>	<b>INITIAL SETUP WLM-1500/2500/3500 .....</b>	<b>13</b>
<b>10</b>	<b>CONFIGURATION WIZARD.....</b>	<b>19</b>
<b>11</b>	<b>BASIC SETTINGS.....</b>	<b>20</b>
<b>12</b>	<b>ADVANCED SETTINGS.....</b>	<b>34</b>
<b>13</b>	<b>FIREWALL SETTINGS .....</b>	<b>49</b>
<b>14</b>	<b>TOOLBOX SETTINGS .....</b>	<b>59</b>

## Introduction

Congratulations on your purchase of the WLM-1500/2500/3500 Wireless ADSL2+ Modem. The WLM-1500 uses technology based on 802.11n, while the WLM-2500/3500 is fully compliant with 802.11n. These modems are also fully compliant with 802.11g & 802.11b. These modems provide the best performance when used in combination with 802.11n client adapters.

The WLM-1500/2500/3500 is not only a Modem or Wireless Access Point, but can also be used to connect wired Ethernet devices.

For data protection and privacy, the WLM-1500/2500/3500 can encode all wireless transmissions with WEP, WPA or WPA2 encryption. By default, the modem is secured with a WPA2 (AES) encryption key. (The WPA2-key is printed on the label underneath the modem.)

With a built-in DHCP Server & powerful SPI firewall the WLM-1500/2500/3500 protects your computers against intruders and known Internet attacks, and also provides safe VPN pass-through.

# 1 Key Features

---

Features	Advantages
<b>IEEE 802.11g compliant</b>	Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices
<b>Based on 802.11n technology</b>	WLM-1500: Up to 3 times faster than regular 802.11g. WLM-2500/3500: Up to 6 times faster than regular 802.11g  (in combination with a 150n or 802.11n wireless adapter)
<b>Four 10/100 Mbps Fast Ethernet Port (Auto-Crossover)</b>	To connect four wired PC's as well.
<b>Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI</b>	Avoids the attacks of Hackers or Viruses from Internet
<b>Supports 802.11i (WPA/WPA2, AES), VPN pass-through</b>	Provide mutual authentication (Client and dynamic encryption keys to enhance security)
<b>Integrated modem (Annex A)</b>	Fully compatible with the fastest ADSL2+ connections up-to-date.

## 2 Package Contents

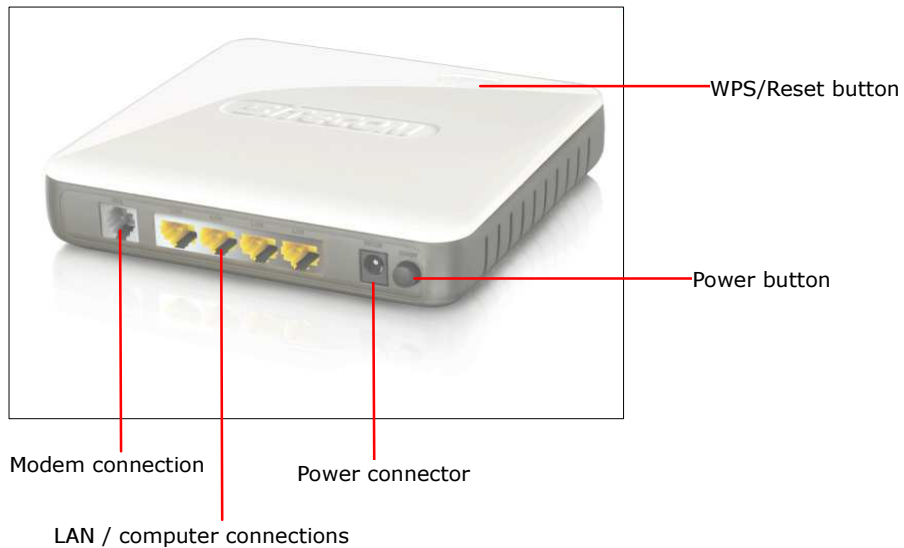
---

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLM-1500/2500/3500 modem/router
2. 220V ~ 240V Power Adapter
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable
7. RJ11 cable

### 3 Product Layout

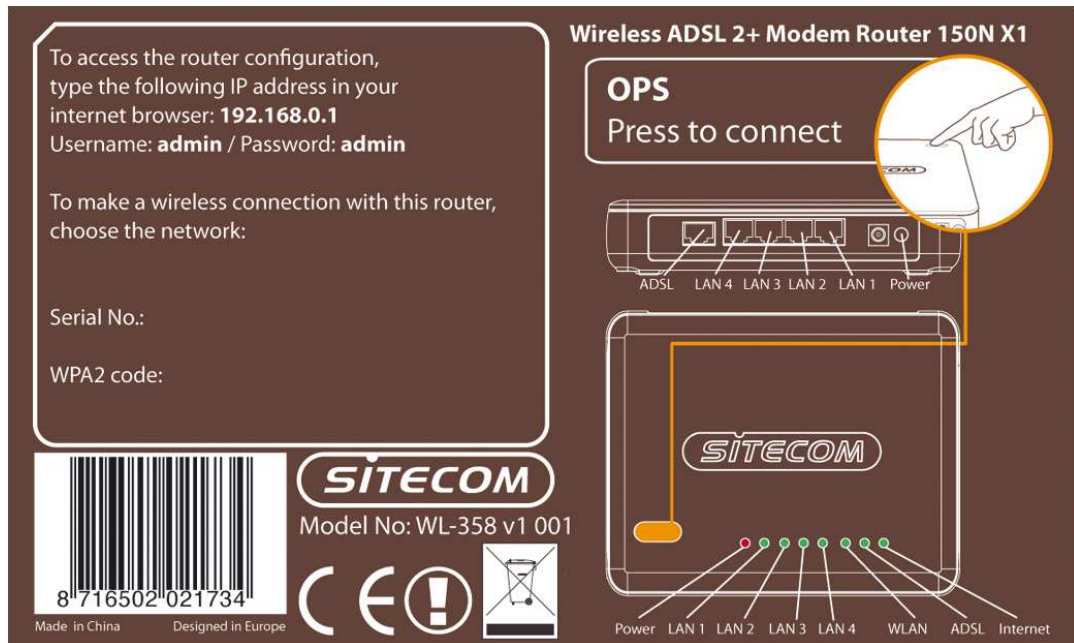
---



Port	Description
<b>ADSL</b>	Connect your telephone/ADSL cable this port
<b>LAN</b>	Connect the cable from your PC or network device to this ports.
<b>Power connector</b>	Connect your power adapter to this port.
<b>Power button</b>	Turn the modem On or Off.

## Back label

The back label describes the corresponding LED indications and port functionality.



LED	Description
<b>Power</b>	Lights up when powered ON. Blinks on TEST/RESET
<b>ADSL</b>	Lights up when an ADSL cable is connected.
<b>Internet</b>	Lights up when internet connection is UP.
<b>WLAN</b>	Lights up in Blue when WLAN is enabled. Blinks on traffic
<b>OPS</b>	Blinks when OPS mode is on
<b>LAN1~4</b>	When a LAN cable is connected the corresponding light lights up.

## **4 System Requirements**

---

To begin using the WLM-1500/2500/3500, make sure you meet the following as minimum requirements:

- PC/Notebook.
- 1 Free Ethernet port.
- Wi-Fi card/USB dongle (802.11 b/g/n) – optional.
- Annex A, ADSL internet connection.
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5 cables.

## **5 WLM-1500/2500/3500 Placement**

---

You can place the WLM-1500/2500/3500 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Modem/Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and the ADSL/phone line should not be over 2 meters long.



## 6 Setup LAN, WAN

---



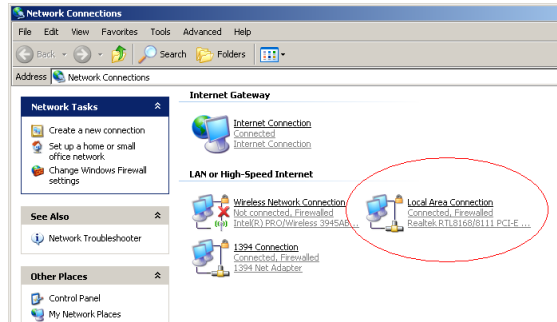
Modem connection

LAN / computer connections

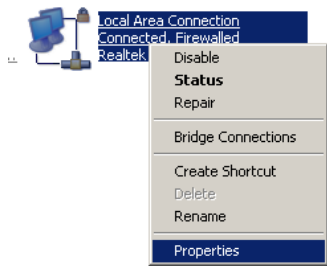
# 7 PC Network Adapter setup

## Windows XP

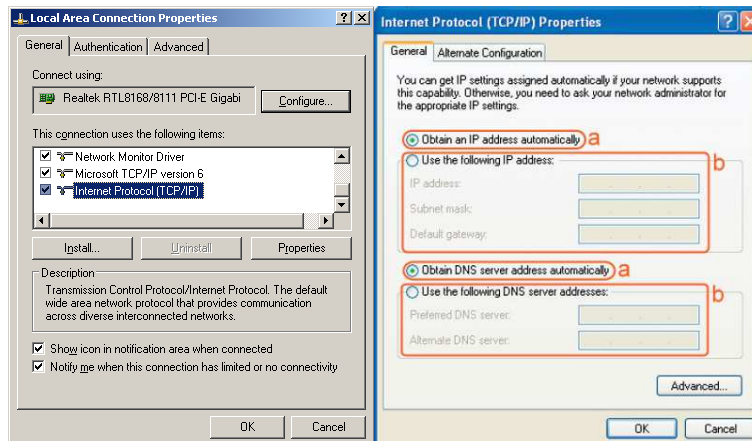
- Go to [Start Menu], → [Control panel], → [Network Connections].



- Right-mouse-click on the [Local Area Connection] icon, and select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].

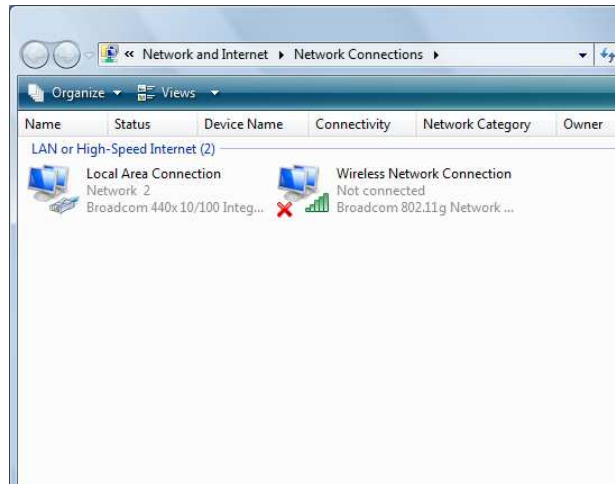


- Select the [General] tab.

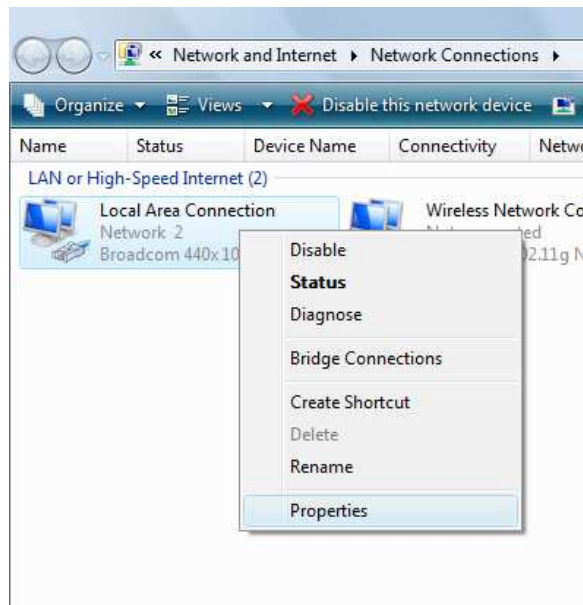
The WLM-1500/2500/3500 supports DHCP. Please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

## Windows Vista/Windows 7

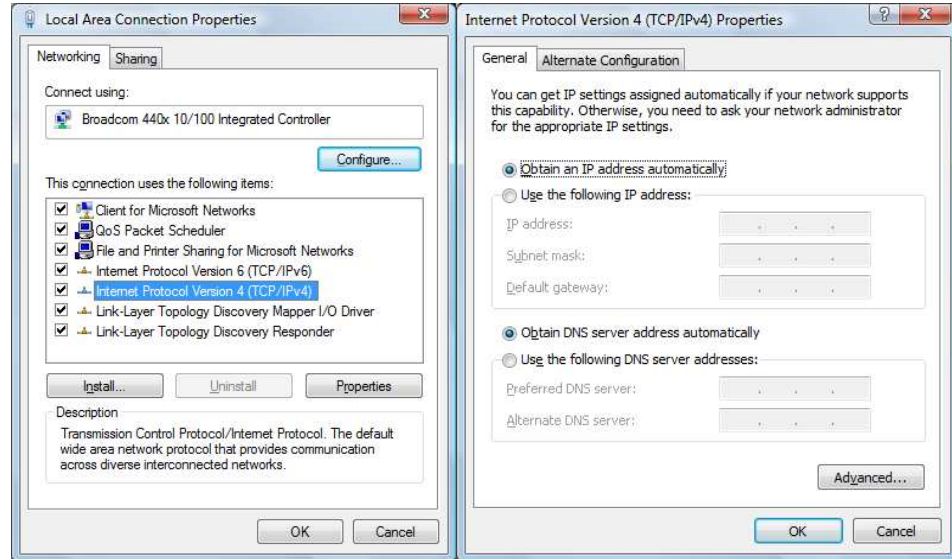
- Go to [Start Menu], → [Control panel], → [View network status and tasks], -> [Manage network connections].



- Right-mouse-click on the [Local Area Connection] icon, and select [properties]



- Select [*Internet Protocol Version 4 (TCP/IPv4)*], and Click [*Properties*].



- Open the [*General*] tab.

The WLM-1500/2500/3500 supports DHCP. Please select both [*Obtain an IP address automatically*] and [*Obtain DNS server address automatically*].

## 8 Bring up the WLM-1500/2500/3500

---

Connect the supplied power-adaptor to the power inlet port and connect it to a wall outlet. Press the Power-Button to turn the modem on.

The WLM-1500/2500/3500 automatically enters the self-test phase. During self-test phase, the Power LED will blink briefly, and then will be lit continuously to indicate that this product is in normal operation.

## 9 Initial Setup WLM-1500/2500/3500

---

### LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).



2. Type <http://192.168.0.1> in address bar and press [Enter]

Type user name and password (The default username is "admin", the password can be found on the back label of the device).



3. Click **OK**.
4. You will see the home page of the WLM-1500/2500/3500.

## Status

The System status section allows you to monitor the current status of your router: the UP time, hardware information, serial number as well as firmware version information is displayed here.

wireless

**modem router**300N

**SITECOM**

[Home](#) | [Setup Wizard](#) | [Basic Settings](#) | [Advanced Settings](#) | [Firewall](#) | [Toolbox](#) | [Choose your language](#)

[Status](#) | [Statistics](#) | [ADSL Statistics](#) | [DHCP List](#) | [QoS Queue](#)

### ADSL Router Status

This page shows the current status and some basic settings of the device

#### System :

Alias Name :	ADSL Modem/Router
Uptime :	2:18
Firmware Version :	1.00g
DSP Version :	2.9.0.4
DNS Server :	
Default Gateway :	

#### DSL :

Operational Status :	ACTIVATING.
Upstream Speed :	0 kbps
Downstream Speed :	0 kbps

#### LAN Configuration :

IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled
MAC Address :	001f1f90f5bc

#### WAN Configuration :

Interface	VPI/VCI	Encap	Protocol	IP Address	Default Gateway	Status
-----------	---------	-------	----------	------------	-----------------	--------

Refresh

## Statistics

You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems. To display statistics for any new data, click "Refresh".

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The page title is "wireless modem router 300N" with the Sitecom logo. The navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. A language selection dropdown is set to "Choose your language". Below the navigation bar, there are tabs for Status, Statistics (selected), ADSL Statistics, DHCP List, and QoS Queue. The Statistics section is titled "Statistics" and includes a note: "This page shows the current status and some basic settings of the device". A table displays network statistics for two interfaces: eth0 and wlan0. The table has columns for Interface, Rx pkt, Rx err, Rx drop, Tx pkt, Tx err, and Tx drop. At the bottom right, there are "Refresh" and "Reset" buttons.

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	1312	0	0	3290	0	0
wlan0	445272	2149	0	7039	0	0

## ADSL Statistics

This page shows the ADSL line statistic information.

wireless

modem router<sub>300N</sub>

SITECOM

Home

Setup Wizard

Basic Settings

Advanced Settings

Firewall

Toolbox

Choose your language ▾

Status

Statistics

ADSL Statistics

DHCP List

QoS Queue

ADSL Statistics

Mode :

Latency :

Trellis Coding : Enable

Status : ACTIVATING.

Power level : L0

Uptime :

Downstream

Upstream

SNR Margin (dB) : 0.0

Attenuation (dB) : 0.0

Output Power (dBm) : 0.0

Attainable Rate (Kbps) : 0

Rate(Kbps) : 0

DTM frame bytes :

RS code word check bytes :

RS code word DMT frame size :

Interleaver depth :

Delay (msec) : >

FEC : 0

CRC : 0

Total ES : 0

Total SES : 0

Total UAS : 0

www.sitecom.com | © 1996 - 2010 Sitecom Europe BV, all rights reserved



## DHCP List

This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

wireless  
**modem router** 300N  
SITECOM

Home Setup Wizard Basic Settings Advanced Settings Firewall Toolbox Choose your language ▾

Status Statistics ADSL Statistics **DHCP List** QoS Queue

**Active DHCP Clients table**

This table shows the assigned IP Address, corresponding MAC Address and expiration time of the connected clients.

IP Address	MAC Address	Expiration time
192.168.0.101	b8:ac:6f:76:bd:1d	429496729
192.168.0.105	00:23:14:ce:79:2c	429496729

Refresh Back

Use the **Refresh** button to update the available information.

## QoS Queue

The screen allows you to configure a QoS queue and assign it to a specific network.

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, there are tabs for Status, Statistics, ADSL Statistics, DHCP List, and QoS Queue. The QoS Queue tab is active, displaying the 'QoS Queue Configuration' section. This section includes a descriptive paragraph about Quality of Service (QoS), a 'Queue config list' table with columns for Interface Name, Queue Description, Precedence, Queue Key Relay Blocking, and Enable, and a configuration form with fields for Queue Description, Queue Status, Queue Interface, and Queue Priority. The form has dropdown menus for the last three fields. 'Apply' and 'Cancel' buttons are at the bottom right.

If the channel operation modes of your ADSL router are not configured and you enable the QoS function, you'll see the following message:

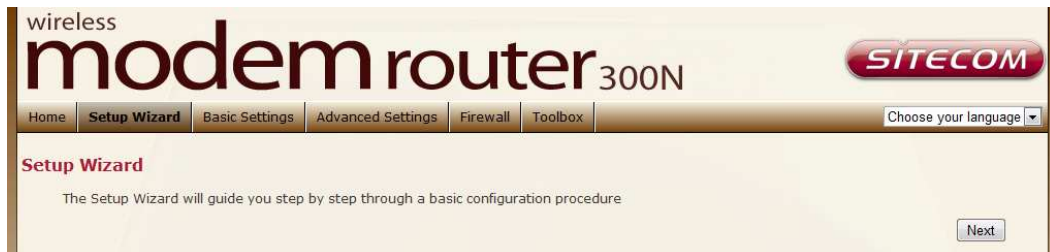


Please follow the Setup Wizard to finish WAN configuration before setting up QoS.

Parameter	Description
Queue Description	The description of the queue will appear automatically according to your selection.
Queue Status	The status of the queue is selected here.
Queue Interface	The WAN interface of the queue is selected here.
Queue Priority	The priority of the queue is selected here.

## 10 Configuration Wizard

Click **Wizard** to configure the modem. The Setup wizard will now be displayed; check that the adsl line is connected and click **Next**.



Select your country from the Country list. Select your internet provider. Click **Next**.



Depending on the chosen provider, you may need to enter your user name and password or hostname in the following window. After you have entered the correct information, click **Next**.

Click **Finish** to complete the configuration.

# 11 Basic Settings

## LAN Settings

This page is used to configure the LAN interface of your ADSL Router. You can set IP address, subnet mask, and IGMP Snooping.

The screenshot shows the 'LAN Settings' page of a Sitecom wireless modem router 300N. The page has a navigation bar with tabs: Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. Below this is a sub-navigation bar with tabs: LAN Settings (selected), DHCP Settings, WAN Settings, Wireless settings, Security Settings, ACL, and WPS. The main content area is titled 'LAN Settings' and contains a description: 'This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc'. Below the description is a form with the following fields: Interface Name (br0), IP Address (192.168.0.1), Subnet Mask (255.255.255.0), IGMP Snooping (Disable), and Ethernet to Wireless Blocking (Disable). An 'Apply' button is located at the bottom right of the form.

Parameter	Description
Interface Name	The interface name is "br0".
IP Address	Enter the IP Address of the ADSL router for the local user to access the router's web page. By default, the IP Address is <b>192.168.0.1</b> .
Subnet Mask	Enter the Subnet Mask of the ADSL router. By default, the Subnet Mask is <b>255.255.255.0</b> .
Secondary IP	Assign second IP address to LAN.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports. When "IGMP Snoop" (Internet Group Management Protocol Snoop) is enabled, the router can make intelligent multicast forwarding decisions by examining the contents of each frame's IP header. Without the function, the router will broadcast the multicast packets to each port and may create excessive traffic on the network and degrade the performance of the network.
Ethernet to Wireless Blocking	Enable/disable the 'Ethernet to Wireless Blocking', when this function is enabled, the traffic between Ethernet and wireless interfaces is not allowed.

## DHCP Settings

You can configure your network and the router to use the Dynamic Host Configuration Protocol (DHCP). This page allows you to select the DHCP mode that this router will support.

There are two different DHCP Modes: DHCP Server and DHCP Relay. When the router is acting as DHCP server, please configure the router in the "DHCP Server" page; while acting as DHCP Relay, you can setup the relay in the "DHCP Relay" page.

The screenshot shows the web interface of a Sitecom modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. Below this is a secondary navigation bar with LAN Settings, DHCP Settings (selected), WAN Settings, Wireless settings, Security Settings, ACL, and WPS. The main content area is titled "DHCP Settings" and contains a sub-header "DHCP Server". The text below the sub-header explains the function of the DHCP Server. The configuration fields are as follows:

DHCP Mode :	<input type="radio"/> None <input type="radio"/> DHCP Relay configuration <input checked="" type="radio"/> DHCP Server	
LAN IP Address :	192.168.0.1	
Subnet Mask :	255.255.255.0	
IP Pool Range :	192.168.0.100 - 192.168.0.200	<input type="button" value="Show Client"/>
Max lease time :	-1	Seconds (-1 indicates an infinite lease)
Domain name :	wk358	
Gateway Address :	192.168.0.1	

At the bottom right of the configuration area are two buttons: "Apply" and "MAC-Base Assignment". The footer of the page contains the text: "www.sitecom.com | © 1996 - 2010 Sitecom Europe BV. all rights reserved".

## DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a user's computer on your network requests Internet access, the router contacts your ISP to obtain the IP configuration, and then forward that information to the computer.

Parameter	Description
<b>DHCP Server Address</b>	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN interface will be passed to the default gateway, which should route the request appropriately.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and go back to the web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## DHCP Server

When the DHCP server is enabled, the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP addresses.

Parameter	Description
<b>LAN IP Address</b>	The current IP Address of the router.
<b>Subnet Mask</b>	The current Subnet Mask of the router.

<b>IP Pool Range</b>	You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default, the IP range is starting from IP 192.168.0.100 to 192.168.0.200.
<b>Show Client</b>	Click this button and a table is displayed. You can know the assigned IP address, MAC address and time expired for each DHCP leased client.
<b>Max Lease Time</b>	In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is terminated.
<b>Domain Name</b>	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.
<b>Gateway Address</b>	The IP address of the ADSL router.
<b>MAC Base Assignment</b>	Click this button and you can assign a static IP Address to the computer with the designated MAC Address. The MAC Address is the 12-digit hexadecimal number, for example "00-d0-59-c6-12-43". The Assigned IP Address should be a unique IP Address.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## WAN Settings

The page allows you to select any combination of DSL modes.

The screenshot shows the WAN Settings page of a Sitecom wireless modem router 300N. The page has a navigation bar with tabs for Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. Below this is a sub-navigation bar with tabs for LAN Settings, DHCP Settings, WAN Settings (selected), Wireless settings, Security Settings, ACL, and WPS. The main content area is titled 'WAN Settings' and includes a description: 'This page is used to configure basic WAN settings like ADSL and DNS settings'. Under the 'ADSL Settings' section, there are several configuration options: 'ADSL modulation' with checkboxes for G.Lite, G.Dmt (checked), T1.413 (checked), ADSL2 (checked), and ADSL2+ (checked); 'AnnexL option' with a checkbox for 'Enabled (Note: Only supported by ADSL 2)'; 'AnnexM option' with a checkbox for 'Enabled (Note: Only supported by ADSL 2/2+)'; and 'ADSL capability' with checkboxes for 'Enable Bitswap' and 'Enable SRA'. An 'Apply' button is located at the bottom right of the page.

Parameter	Description
<b>ADSL modulation</b>	Choose preferred ADSL standard protocols.
<b>Annex L Option</b>	Enable/Disable ADSL2/ADSL2+ Annex L capability.
<b>Annex M Option</b>	Enable/Disable ADSL2/ADSL2+ Annex M capability.
<b>ADSL Capability</b>	<b>Bitswap Enable</b> – Enable/Disable bitswap capability.
	<b>SRA Enable</b> – Enable/Disable SRA (seamless rate adaptation) capability.
<b>ADSL Tone</b>	Choose tones to be masked. The masked tones will not carry any data. Click "Tone Mask" to mask the tone number you have selected or all the tone numbers.

When you finish, click '**Apply**'. You'll see the following message displayed on the web browser:



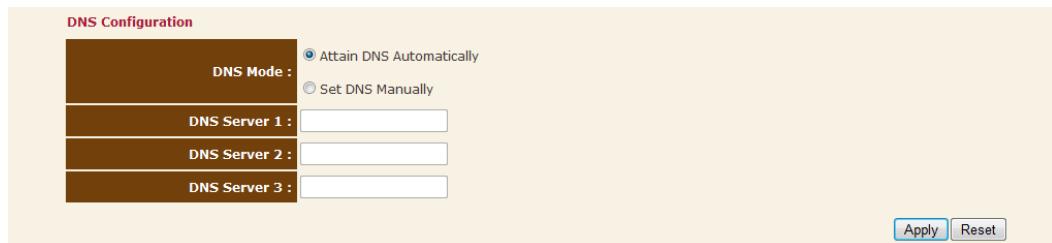
Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the



settings will take effect after it reboots.

## DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as "www.router.com", a DNS server will find that name in its index and the matching IP address. This page is used to select the way to obtain the IP addresses of the DNS servers.



The screenshot shows the 'DNS Configuration' page. It has a title 'DNS Configuration' in red. Below it, there's a section with a dark brown background. On the left, it says 'DNS Mode :'. To the right, there are two radio buttons: 'Attain DNS Automatically' (which is selected) and 'Set DNS Manually'. Below this, there are three input fields labeled 'DNS Server 1 :', 'DNS Server 2 :', and 'DNS Server 3 :'. At the bottom right of the page, there are two buttons: 'Apply' and 'Reset'.

Parameter	Description
<b>Attain DNS Automatically</b>	Select this item if you want to use the DNS servers obtained from ISP.
<b>Set DNS Manually</b>	Select this item to specify up to three DNS IP addresses.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## Wireless Settings

This section provides the wireless network settings for your router. You can enable the wireless AP function here.

The screenshot shows the 'Wireless Basic Settings' page of a Sitecom modem router 300N. The page has a navigation bar with tabs: Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. Below this is a sub-navigation bar with tabs: LAN Settings, DHCP Settings, WAN Settings, Wireless settings (selected), Security Settings, ACL, and WPS. The main content area is titled 'Wireless Basic Settings' and includes a description: 'This page is used to configure the parameters for the wireless LAN like wireless encryption settings, channel and band.' There is a checkbox labeled 'Disable Wireless LAN Interface' which is unchecked. Below this are several configuration fields: Band (2.4 GHz (B+G+N)), Mode (AP), SSID (Sitecom90f5bc), Channel width (40MHz), Sideband (Upper), Channel (11), Radio Power (mW) (60 mW), and Associated Clients (Show Active Clients). An 'Apply' button is at the bottom right.

Parameter	Description
<b>Band</b>	<p>Please select the radio band from one of the following options.</p> <p>2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps).</p> <p>2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps).</p> <p>2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).</p> <p>2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps).</p> <p>2.4 GHz (G+N):2.4GHz band, only allows 802.11g and 802.11n wireless network client to connect this router (maximum transfer rate 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).</p> <p>2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b,</p>

<b>Mode</b>	802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients). It allows you to set the router to act in "AP", "Client" or "WDS" mode.
<b>SSID</b>	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the router is "default".
<b>Channel Width</b>	Set channel width of wireless radio. Do not modify default value if you don't know what it is, default setting is 'Auto 20/40 MHz'.
<b>Control Sideband</b>	Select the upper band or lower band for your radio frequency. While upper band is selected, the channel number you can select is from channel 5 to channel 11. While lower band is selected, the channel number you can select is from channel 1 to channel 7.
<b>Channel Number</b>	It is the radio channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel. Please select the country you are located and designate a channel that the router will use. If you want to let the router automatically to find an available channel with the highest signal strength, please select "Auto".
<b>Radio Power (mW)</b>	Set the maximum output power of the router. The higher output power, the wider coverage range.
<b>Associated Clients</b>	Click "Show Active Clients" button and you can see the wireless clients connected to the router.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## Security

This router provides complete wireless LAN security functions, include WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

wireless  
**modem router** 300N  
SITECOM

Home Setup Wizard **Basic Settings** Advanced Settings Firewall Toolbox Choose your language ▼

LAN Settings DHCP Settings WAN Settings Wireless settings **Security Settings** ACL WPS

**Wireless Security Settings**

Because we value your security we have set your network by default to WPA2 security. You can change those settings here, however we strongly advise you to keep these settings intact if you are not knowledgeable.

Encryption : WPA2 Mixed Set Key

802.1x Authentication : ☐ WEP 64bits ☐ WEP 128bits

WPA Mode : ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

Pre-Shared Key Format : Passphrase

Pre-Shared Key : \*\*\*\*\*

RADIUS Server : Port 1812 IP address 0.0.0.0 password

When encryption WEP is selected, you must set WEP key value.

Apply

Parameter	Description
<b>Encryption</b>	<p>You can choose "None" to disable the encryption or select "WEP", "WPA(TKIP)", "WPA2(AES)" or "WPA2 Mixed" mode for security. When "WEP" is enabled, please click "Set WEP Key" button to choose the default key and set the four sets of WEP keys.</p> <p><b>WEP</b> –WEP is less level of security than WPA. WEP supports 64-bit and 128-bit key lengths to encrypt the wireless data.</p> <p><b>WPA(TKIP)</b> – WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.</p> <p><b>WPA2(AES)</b> – WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption.</p> <p><b>WPA Mixed</b> – The router supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.</p>
<b>Use 802.1x Authentication</b>	<p>IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed</p>

	by a RADIUS server. Check this box to authenticates user by IEEE 802.1x.
<b>WEP-64Bits</b>	WEP is less level of security than WPA. WEP supports 64-bit and 128-bit key lengths to encrypt the wireless data. The longer key length will provide higher security. When "WEP-64Bits" is selected, you have to enter exactly 5 ASCII characters ("a-z" and "0-9") or 10 hexadecimal digits ("0-9", "a-f") for each Key (1-4).
<b>WEP-128Bits</b>	When "WEP-128Bits" is selected, you have to enter exactly 13 ASCII characters ("a-z" and "0-9") or 26 hexadecimal digits ("0-9", "a-f") for each Key (1-4).
<b>WPA Authentication Mode</b>	There are two types of authentication mode for WPA. <b>Enterprise (RADIUS)</b> – It uses an external RADIUS server to perform user authentication. To use RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to "Authentication RADIUS Server" setting below for RADIUS setting.
<b>Pre-Shared Key Format</b>	<b>Personal (Pre-Shared Key)</b> – Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively. You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: "iamguest" Hexadecimal Digits: "12345abcde"
<b>Pre-Shared Key Authentication RADIUS Server</b>	Please enter 8-63 characters as the "Pre-Shared Key". Enter the port (default is 1812), the IP address and the password of external RADIUS server are specified here.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.

The screenshot shows the web interface of a SITEMCOM wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, a sub-menu shows LAN Settings, DHCP Settings, WAN Settings, Wireless settings (selected), Security Settings, ACL (selected), and WPS. The main content area is titled "Wireless Access Control" and contains the following elements:

- A descriptive paragraph: "If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point."
- A "Wireless Access Control Mode:" label with a dropdown menu currently set to "Disable" and an "Apply" button.
- An "Add MAC Address. :" section with a "MAC Address :" input field (placeholder: "ex. 00E086710502") and "Add" and "Reset" buttons.
- A "Current Access Control List :" section with a table header showing "MAC Address" and "Select" columns. Below the header are "Delete selected" and "Delete all" buttons.

Parameter	Description
<b>Wireless Access Control Mode</b>	<p>This router can prevent the wireless clients from accessing the wireless network by checking the MAC Address of the clients. If you enable this function, please set the MAC Address of the wireless clients that you want to filter.</p> <p><b>Disable</b> – Disable this function.</p> <p><b>Allow Listed</b> – Only allow the wireless clients with the MAC Address you have specified can access to the router.</p> <p><b>Deny Listed</b> – The wireless clients with the MAC Address you have specified will be denied accessing to the router.</p>
<b>MAC Address</b>	Enter the MAC Address of the wireless clients for the filtering control.
<b>Current Access Control List</b>	If you want to remove some MAC address from the "Current Access Control List ", select the MAC addresses you want to remove in the list and then click "Delete Selected". If you want remove all MAC addresses from the table, just click "Delete All"

button. Click "Reset" will clear your current selections.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## WPS

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management.

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network.

This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below.

The screenshot shows the 'WPS' configuration page of a Sitecom modem router 300N. The page has a navigation bar with tabs: Home, Setup Wizard, Basic Settings (selected), Advanced Settings, Firewall, and Toolbox. Below this is a sub-navigation bar with tabs: LAN Settings, DHCP Settings, WAN Settings, Wireless settings, Security Settings, ACL, and WPS (selected). The main content area is titled 'Wi-Fi Protected Setup' and includes a description: 'This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.' There are three main sections: 1. 'Disable WPS' with a checkbox. 2. 'WPS Status' with radio buttons for 'Configured' and 'UnConfigured' (selected). 3. 'Self-PIN Number' with a text field containing '12345670' and a 'Regenerate PIN' button. Below these is a 'Push Button Configuration' section with a 'Start PBC' button. At the bottom, there is a 'Client PIN Number' section with a text field and a 'Start PIN' button. 'Apply' and 'Reset' buttons are located on the right side of the page.

Parameter	Description
<b>Disable WPS</b>	Check to disable the Wi-Fi protected Setup.
<b>WPS Status</b>	When AP's settings are factory default (out of box), it is set to open security and un-configured state. "WPS Status" will display it as "UnConfigured". If it already shows "Configured", some registrars such as Vista WCN will not configure AP. Users will need to go to the "Backup/Restore" page and click "Reset" to reload factory default settings.
<b>Self-PIN Number</b>	"Self-PIN Number" is AP's PIN. Whenever users want to change AP's PIN, they could click "Regenerate PIN" and then click " Apply Changes". Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click " Apply Changes". However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.



<b>Regenerate PIN</b>	Click to regenerate the Self-PIN Number.
<b>Push Button</b>	Clicking this button will invoke the PBC method of WPS. It is only used when AP acts as a registrar.
<b>Configuration</b>	Click to start the Push Button method of WPS.
<b>Start PBC</b>	Click to start the Push Button method of WPS.
<b>Reset</b>	It restores the original values.
<b>Client PIN Number</b>	It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with checksum error, there will be a warning message popping up. If users insist on this PIN, AP will take it.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

# 12      Advanced Settings

## Wireless Settings

This page allows advanced users who have sufficient knowledge of wireless LAN. These setting shall not be changed unless you know exactly what will happen for the changes you made on your router.

wireless

modemrouter300N

SITECOM

Home

Setup Wizard

Basic Settings

Advanced Settings

Firewall

Toolbox

Choose your language

Wireless settings

QoS

UPnP

IGMP

Routing

SNMP

DDNS

RIP

Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type :

☐ ping statistics

☐ Pre-Shared Key

☒ Auto

Fragment Threshold :

2346

(256-2346)

RTS Threshold :

2347

(0-2347)

Beacon Interval :

100

(20-1024 ms)

Data Rate :

Auto

Preamble Type :

☒ Long Preamble

☐ Short Preamble

Broadcast SSID :

☒ Enable

☐ Disable

Queue Key Relay Blocking :

☐ Enable

☒ Disable

Protection :

☐ Enable

☒ Disable

Aggregation :

☒ Enable

☐ Disable

Short GI :

☒ Enable

☐ Disable

Apply

www.sitecom.com | © 1996 - 2010 Sitecom Europe BV, all rights reserved

Parameter	Description
Authentication Type	There are three authentication types: "Open System", "Shared Key" and "Auto".  Open System: Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.  Shared Key: Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of

the WEP privacy mechanism.

	<p>Auto: Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.</p>
<b>Fragmentation Threshold</b>	<p>Fragment Threshold specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance. Enter a value from 256 to 2346.</p>
<b>RTS Threshold</b>	<p>This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset "RTS threshold" size, the RTS/CTS mechanism will not be enabled. The wireless router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.</p>
<b>Beacon Interval</b>	<p>The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network. The range for the beacon period is between 20 and 1024 with a default value of 100 (milliseconds).</p>
<b>Data Rate</b>	<p>The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select <i>Auto</i> to have the wireless router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the router and a wireless client. The default setting is "Auto".</p>
<b>Preamble Type</b>	<p>The Preamble Type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless stations. Make sure to select the appropriate preamble type. Note that high network traffic areas should use the "Short Preamble". CRC is a common technique for detecting data transmission errors.</p>
<b>Broadcast SSID</b>	<p>If this option is enabled, the router will automatically transmit the network name (SSID) into open air at regular interval. This feature is intended to allow clients to dynamically discover the router. If this option is disabled, the router will hide its SSID. When this is done, the clients cannot directly discover the router and MUST be configure with the SSID for accessing to the router. It is used to protect your network from being accessed easily.</p>
<b>Relay Blocking Protection</b>	<p>When you enable this function, wireless clients will not be able to directly access other wireless clients. This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g/802.11n wireless stations. When the</p>

<b>Aggregation</b>	protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted. This function is used to join multiple data packets for transmission as a single unit to increase network efficiency.
<b>Short GI</b>	The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. Enable this function will increase network efficiency.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

# QoS

The router supports IP QoS feature that can provide different priority to different users or data flows.

## Classification

Classification

Configuration of classification table for IPQoS.

IP QoS : ☒ Disable ☐ Enable

Current Auto-PVC Table : IP Pred

Apply

Specify Traffic Classification Rules. :

Source IP :

Subnet Mask :

Port :

Destination IP :

Subnet Mask :

Port :

Protocol :

Physical Port :

Classification Results :

ClassQueue : Click to Select

802.1p\_Mark :

IP.Pred\_Mark :

TOS\_Mark :

Add

IP QoS Rules :

		classification Rules						Classification Results				
Select	Status	Src IP	Src Port	Dst IP	Dst Port	Protocol	Lan Port	Interface	Priority	IP Pred	IP TOS	802.1p

Delete selected

Delete all

Parameter	Description
IP QoS	Click the radio button to enable or disable the IP QoS function.
Default QoS	Select the default mode of QoS from the list.  IP Pred: In QoS, a three-bit field in the ToS byte of the IP header (see RFC 791). Using IP Precedence, a network administrator can assign values from 0(the default) to 7 to classify and prioritize types of traffic.  802.1P: IEEE 802.1p is a 3 bit field within an Ethernet frame header when using tagged frames on an 802.1 network. It specifies a priority value of between 0 and 7 inclusive that can be used by Quality of Service (QoS) disciplines to differentiate traffic.
Source IP	The IP address of the traffic source.
Netmask (Source)	The source IP netmask. This field is required if the source IP has been entered.
Port (Source)	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination IP	The IP address of the traffic destination.
Netmask	The destination IP netmask. This field is required if the

<b>(Destination) Port (Destination)</b>	destination IP has been entered. The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
<b>Protocol</b>	The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.
<b>Physical Port</b>	The incoming ports. The selections include LAN ports, wireless port, and the blank for not applicable.
<b>ClassQueue</b>	The priority level for the traffic that matches this classification rule. Please refer to <b>5.2.5.2 QoS Queue</b> to create a ClassQueue.
<b>802.1p_Mark</b>	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that matches this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.
<b>IP.Pred_Mark</b>	Select this field to mark the IP precedence bits in the packet that match this classification rule.
<b>TOS_Mark</b>	The IP (Internet Protocol) uses the ToS (Type of Service) field to provide an indication of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting an IP datagram through a particular network.0
<b>IP QoS Rules</b>	This table lists the rules you have configured. Click "Delete Selected" to delete the selected rules or click "Delete All" to delete all the rules.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## UPnP

When the UPnP function is enabled, the router can be detected by UPnP compliant system such as Windows XP. The router will be displayed in the Neighborhood of Windows XP, so you can directly double click the router or right click the router and select "Invoke" to configure the router through web browser.



The screenshot shows the web management interface of a Sitecom Modem Router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings (which is selected), Firewall, and Toolbox. Below this, there are tabs for various settings: Wireless settings, QoS, UPnP (which is selected), IGMP, Routing, SNMP, DNS, and RIP. The main content area is titled "UPnP Configuration" and contains the following text: "This page is used to configure UPnP. The system acts as a daemon when you enable it. Select the WAN interface (upstream) that will use UPnP." Below the text, there are two configuration options: "UPnP" with radio buttons for "Disable" (selected) and "Enable", and "WAN Interface" with a drop-down menu. An "Apply" button is located at the bottom right of the configuration area.

Parameter	Description
<b>UPnP</b>	Enable or disable UPnP feature.
<b>WAN Interface</b>	The upstream WAN interface is selected here. Select WAN interface that will use UPnP from the drop-down lists.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## IGMP

The IGMP Proxy page allows you to enable multicast on WAN and LAN interfaces. The LAN interface is always served as downstream IGMP proxy, and you can configure one of the available WAN interfaces as the upstream IGMP proxy. Upstream is the interface that IGMP requests from hosts are sent to the multicast router. Downstream is the interface data from the multicast router are sent to hosts in the multicast group database.

The screenshot shows the web interface of a Sitecom Modem Router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings (which is highlighted), Firewall, and Toolbox. Below this, there's a sub-navigation bar with links for Wireless settings, QoS, UPnP, IGMP (which is highlighted), Routing, SNMP, DDNS, and RIP. The main content area is titled 'IGMP Proxy Configuration'. It contains a paragraph explaining the IGMP proxy feature. Below the text, there are two configuration options: 'IGMP Proxy' with radio buttons for 'Disable' and 'Enable' (where 'Enable' is selected), and 'Proxy Interface' with a dropdown menu. An 'Apply' button is located at the bottom right of the configuration area.

Parameter	Description
<b>IGMP Proxy</b>	Enable or disable IGMP proxy feature.
<b>Proxy Interface</b>	The upstream WAN interface is selected here.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.



## Routing

The page enables you to define specific route for your Internet and network datas.

Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the router provide the most appropriate path for all your Internet traffic.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

wireless  
**modem router** 300N  
SITECOM

Home Setup Wizard Basic Settings **Advanced Settings** Firewall Toolbox Choose your language ▾

Wireless settings QoS UPnP IGMP **Routing** SNMP DDNS RIP

**Routing Configuration**

This page is used to configure the routing information. Here you can add/delete IP routes.

☒ **Enable**

Destination :

Subnet Mask :

Next Hop :

Metric :

Interface : any ▾

Apply Update Delete selected Show routes

**Static Route Table :**

Select	State	Destination	Subnet Mask	Next Hop	Metric	IF
--------	-------	-------------	-------------	----------	--------	----

Parameter	Description
<b>Enable</b>	Check to enable the selected route or route to be added.
<b>Destination</b>	The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
<b>Subnet Mask</b>	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
<b>Next Hop</b>	The IP address of the next hop through which traffic will flow towards the destination subnet.
<b>Metric</b>	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
<b>Interface</b>	The WAN interface to which a static routing subnet is to be applied.
<b>Add Route</b>	Add a user-defined destination route.

**Show Routes  
Static Route  
Table**

Click this button to view the router's routing table.  
Click "Update" to update the selected destination route on the "Static Route Table". Click "Delete Selected" to delete a selected destination route on the Static Route Table.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## SNMP

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The router can be managed locally or remotely by SNMP protocol.

Parameter	Description
<b>SNMP</b>	Select "Disable" or "Enable" to disable or enable the SNMP feature.
<b>System Description</b>	Enter the system description of the router.
<b>System Contact</b>	Enter the contact person and/or contact information for the router.
<b>System Name</b>	Assign an administratively name for the router.
<b>System Location</b>	The physical location of the router.
<b>System Object ID</b>	It is the vendor object identifier. The vendor's authoritative identification of the network management subsystem contained in the entity.
<b>Trap IP Address</b>	Destination IP address of the SNMP trap.
<b>Community name (read-only)</b>	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
<b>Community name (write-only)</b>	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:

**Change setting successfully!**

Continue

Apply

Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## DDNS

Dynamic DNS (DDNS) allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers.

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings (which is selected), Firewall, and Toolbox. A language selection dropdown is on the right. Below the navigation bar, a sub-menu contains links for Wireless settings, QoS, UPnP, IGMP, Routing, SNMP, DDNS (which is selected), and RIP. The main content area is titled 'Dynamic DNS Configuration' and contains instructions: 'This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.' There is a checkbox labeled 'Disable' which is checked. Below this are three main sections: 'DDNS provider' with a dropdown menu showing 'DynDNS.org', 'Hostname' with a text input field, 'DynDns Settings' with 'Username' and 'Password' text input fields, and 'TZO Settings' with 'Email' and 'Key' text input fields. At the bottom right of the form are three buttons: 'Add', 'Modify', and 'Delete'.

Parameter	Description
<b>Enable</b>	Check the box to enable DDNS function.
<b>DDNS Provider</b>	Select your DDNS service provider here. This router supports DynDNS and TZO service providers
<b>Host Name</b>	Enter the domain name you've obtained from DDNS service provider.
<b>DynDns Settings</b>	
<b>Username</b>	Enter the username assigned by the DDNS service provider.
<b>Password</b>	Enter the password assigned by the DDNS service provider.
<b>TZO Settings</b>	
<b>Email</b>	Enter the Email account that your DDNS service provider assigned to you.
<b>Key</b>	Enter the password that your DDNS service provider assigned to you.
<b>Add/Modify/Remove</b>	These buttons are for you to maintain the DDNS table.-
<b>Dynamic DDNS Table</b>	The DDNS you have configured will be added to the list.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:

**Change setting successfully!**

Continue

Apply

Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

Most small home or office networks do not need to use RIP; they have only one router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the ADSL Router). The ADSL Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

Interface :

Receive Mode :

Send Mode :

**RIP Config Table**

Select	Interface	Receive Mode	Send Mode
<input type="checkbox"/>	br0	None	None

Parameter	Description
<b>RIP</b>	Enable/disable the RIP feature.
<b>Interface</b>	Select the interface that you want to enable the RIP feature.
<b>Receive Mode</b>	Indicate the RIP version in which information must be

**Send Mode**

passed to the DSL device in order for it to be accepted into its routing table.

**RIP Config Table**

Indicate the RIP version this interface will use when it sends its route information to other devices.

The RIP you have configured will be listed in the table. If you want to delete some settings, please select the settings and click "**Delete Selected**".

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.



# 13 Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

## Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.

The screenshot shows the 'Port Forwarding' configuration page. At the top, there are tabs for 'Home', 'Wizard', 'Basic Settings', 'Advanced Settings', 'Firewall', and 'Toolbox'. The 'Firewall' tab is selected, and within it, the 'Port Forwarding' sub-tab is active. Below the tabs, there is a 'Port Forwarding' section with a description: 'Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.' Below this, there are radio buttons for 'Disable' (selected) and 'Enable'. To the right is an 'Apply' button. Below the radio buttons, there are input fields for 'Protocol' (set to 'Both'), 'Local IP Address', 'Remote IP-address', 'Interface' (set to 'any'), 'Comment', 'Local Port', and 'Public Port'. There is also an 'Add' button. At the bottom, there is a 'Current Port Forwarding Table' with a table header: 'Select', 'Local IP Address', 'Protocol', 'Local Port', 'Comment', 'Enable', 'Remote Host', 'Public Port', 'Interface'. Below the header, there are 'Delete selected' and 'Delete all' buttons.

Parameter	Description
<b>Port Forwarding</b>	Check this item to enable or disable the port-forwarding feature.
<b>Protocol</b>	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "Both" to forward both "TCP" and "UDP" packets.
<b>Comment</b>	Enter the comment for the setting.
<b>Enable</b>	Check this item to enable this entry.
<b>Local IP Address</b>	IP address of your local server that will be accessed by Internet.
<b>Local IP Port</b>	The destination port number that is made open for this application on the LAN side.
<b>Remote IP Address</b>	The source IP address from which the incoming traffic is allowed. Leave blank for all.

<b>Public Port</b>	The destination port number that is made open for this application on the WAN side
<b>Interface</b>	Select the WAN interface on which the port-forwarding rule is to be applied.
<b>Current Port Forwarding Table</b>	If you want to remove the port forwarding settings from the table, select the items and then click "Delete Selected". If you want remove all settings, just click "Delete All" button.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## Port Filter

The IP/Port filtering feature allows you to deny/allow specific services or applications in the forwarding path.

The screenshot shows the 'Port Filter' configuration page in the Sitecom modemrouter 300N web interface. The page has a navigation bar with links: Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall (selected), and Toolbox. A language dropdown is on the right. Below the navigation bar are tabs for Port Forwarding, Port Filter (selected), MAC filter, URL blocking, Domain blocking, Access Control List, and DMZ. The main content area is titled 'IP/Port Filtering' and includes a description: 'Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' It features two sections for default actions: 'Outgoing Default Action' with radio buttons for Deny and Allow (Allow is selected), and 'Incoming Default Action' with radio buttons for Deny and Allow (Deny is selected). Below these are input fields for a new rule: Direction (Outgoing), Protocol (TCP), Rule Action (Outgoing), Source IP, Subnet Mask, Port, Destination IP, Subnet Mask, and Port. An 'Apply' button is on the right. At the bottom, there is a 'Current Filter Table' with columns: Select, Direction, Protocol, Src Address, Src Port, Dst Address, Dst Port, and Rule Action. Below the table are 'Delete selected' and 'Delete all' buttons. The footer contains the text: 'www.sitecom.com | © 1996 - 2010 Sitecom Europe BV, all rights reserved'.

Parameter	Description
<b>Outgoing Default Action</b>	Specify the default action on the LAN to WAN (Traffic to Internet) forwarding path. You can choose 'Allow' if you allow the IP Addresses listed in the following table to connect to the Internet; choose 'Deny' if you deny the IP Addressed listed in the following table to connect to the Internet.
<b>Incoming Default Action</b>	Specify the default action on the WAN to LAN (Traffic from Internet) forwarding path. You can choose 'Allow' if you allow the IP Addresses listed in the following table from connecting to the Internet; choose 'Deny' if you deny the IP Addressed listed in the following table from connecting to the Internet.
<b>Direction</b>	Select the traffic forwarding direction: outgoing or incoming.
<b>Protocol</b>	There are 3 options available: TCP, UDP and ICMP.
<b>Rule Action</b>	Deny or allow traffic when matching this rule.
<b>Source IP Address</b>	Enter the start IP Address which will be monitored.
<b>Subnet Mask</b>	Enter the Subnet Mask based on the Source IP

<b>Port</b>	Address. LAN users use port number to distinguish one network application over another such as 21 is for FTP service. The port number range is from 0 to 65535. It is recommended that this option be configured by an advanced user.
<b>Destination IP Address</b>	Enter the destination IP Address which will be monitored.
<b>Subnet Mask</b>	Enter the Subnet Mask based on the Destination IP Address.
<b>Port</b>	This is the port or port ranges that define the application.
<b>Current Filter Table</b>	If you want to remove some IP/Port filter settings from the "Current Filter Table", select the items you want to remove in the list and then click "Delete Selected". If you want remove all the items from the table, just click "Delete All" button.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## MAC Filtering

The MAC filtering feature allows you to define rules to allow or deny frames through the router based on source MAC address, destination MAC address, and traffic direction.

wireless  
**modem router** 300N  
SITECOM

Home | Setup Wizard | Basic Settings | Advanced Settings | **Firewall** | Toolbox | Choose your language ▾

Port Forwarding | Port Filter | **MAC filter** | URL blocking | Domain blocking | Access Control List | DMZ

**MAC Filtering**  
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Outgoing Default Action :** ☐ Deny ☒ Allow

**Incoming Default Action :** ☐ Deny ☒ Allow

Direction :

Rule Action : ☒ Deny ☐ Allow

Source MAC Address :

Destination MAC Address :

Apply

Add

**Current Filter Table :**

Select	Direction	Src MAC Address	Dst MAC Address	Rule Action
--------	-----------	-----------------	-----------------	-------------

Parameter	Description
<b>Outgoing Default Action</b>	Specify the default action on the LAN to WAN (Traffic to Internet) forwarding path. You can choose 'Allow' if you allow the IP Addresses listed in the following table from connecting to the Internet; choose 'Deny' if you deny the IP Addressed listed in the following table from connecting to the Internet.
<b>Incoming Default Action</b>	Specify the default action on the WAN to LAN (Traffic from Internet) forwarding path. You can choose 'Allow' if you allow the IP Addresses listed in the following table from connecting to the Internet; choose 'Deny' if you deny the IP Addressed listed in the following table from connecting to the Internet.
<b>Direction</b>	Specify the default action on the WAN to LAN (Traffic from Internet) forwarding path. You can choose 'Allow' if you allow the IP Addresses listed in the following table from connecting to the Internet; choose 'Deny' if you deny the IP Addressed listed in the following table from connecting to the Internet.
<b>Rule Action</b>	Traffic bridging/forwarding direction: outgoing or incoming.
<b>Source MAC Address</b>	Deny or allow traffic when matching this rule.
	The source MAC address. It must be 12-digit hexadecimal format, for example: "00-d0-59-c6-12-43".

**Destination MAC Address**

The destination MAC address. It must be 12-digit hexadecimal format, for example: "00-d0-59-c6-12-50".

**Current Filter Table**

If you want to remove some filter rules from the "Current Filter Table", select the MAC Address you want to remove in the table and then click "Delete Selected". If you want remove all settings from the table, just click "Delete All" button.

---

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## URL Blocking

This page is used to block some URL addresses or keywords.

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. The 'Firewall' tab is selected, and within it, the 'URL blocking' sub-tab is active. The page title is 'URL Blocking Configuration'. A description states: 'This page is used to configure the Blocked FQDN(Such as tw.yahoo.com) and filtered keywords. Here you can add/delete FQDN and filtered keywords.' There are two radio buttons for 'URL Blocking': 'Disable' (selected) and 'Enable'. An 'Apply' button is to the right. Below this is a 'Full domain name' input field with an 'Add' button. The 'URL Blocking Table' has a header with 'Select' and 'FQDN' columns, and buttons for 'Delete selected' and 'Delete all'. Below that is a 'Keyword' input field with an 'Add' button. The 'Keyword Filtering Table' has a header with 'Select' and 'Select Filtered Keyword' columns.

Parameter	Description
<b>URL Blocking</b>	Enable or disable the URL blocking function.
<b>FQDN</b>	Enter FQDN which you want to block. A FQDN is a complete DNS name. For example, "www.yahoo.com".
<b>URL Blocking Table</b>	The FQDN settings will be listed in the table. If you want to delete some FQDN settings from the table, please select the settings and click " <b>Delete Selected</b> ". If you want remove all settings from the table, just click " <b>Delete All</b> " button.
<b>Keyword</b>	Enter the keyword of the URL Address that you want to filter.
<b>Keyword Filtering Table</b>	The keyword settings will be listed in the table. If you want to delete some keyword settings from the table, please select the settings and click " <b>Delete Selected</b> ". If you want remove all settings from the table, just click " <b>Delete All</b> " button.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## Domain Blocking

The firewall includes the ability to block access to specific domain based on string matches. For example, if the URL of Taiwan Yahoo web site is "tw.yahoo.com" and you enter "yahoo.com", the firewall will block all the DNS queries with "yahoo.com" string. So the Host will be blocked to access all the URLs belong to "yahoo.com" domain. That means you can protect your computer, your house, your office and anything else that uses DNS from being able to service domains that you don't want to load.

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. The 'Firewall' tab is selected, and within it, the 'Domain blocking' sub-tab is active. The page title is 'Domain Blocking Configuration'. A message states: 'This page is used to configure the Blocked domain. Here you can add/delete the blocked domain.' Below this, there is a 'Domain Blocking' section with radio buttons for 'Disable' (selected) and 'Enable'. An 'Apply' button is to the right. Underneath is a 'Domain' input field with an 'Add' button. At the bottom, there is a 'Domain Block Table' with two columns: 'Select' and 'Domain'. Below the table are 'Delete selected' and 'Delete all' buttons.

Parameter	Description
<b>Domain Blocking</b>	Check this item to enable the Domain Blocking feature.
<b>Domain</b>	The blocked domain. If the URL of Taiwan Yahoo web site is tw.yahoo.com, the domain can be yahoo.com.
<b>Delete Selected/All</b>	If you want to delete a specific Domain Block entry, check the 'select' box of the Domain Block you want to delete, then click 'Delete Selected' button. If you want remove all settings from the table, just click "Delete All" button.



## ACL Configuration

The Access Control List (ACL) is a list of permissions attached to the router. The list specifies who is allowed to access this router. If ACL is enabled, all hosts cannot access this router except for the hosts with IP address in the ACL table.

wireless  
**modemrouter**<sub>300N</sub> **SITECOM**

Home | Setup Wizard | Basic Settings | Advanced Settings | **Firewall** | Toolbox | Choose your language ▾

Port Forwarding | Port Filter | MAC filter | URL blocking | Domain blocking | **Access Control List** | DMZ

**ACL Configuration**

This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.

**ACL Capability :** ☒ Disable ☐ Enable Apply

**Enable** ☒

**Interface :** LAN ▾

**IP Address :**

**Subnet Mask :**

Add

**ACL Table :**

Select	State	Interface	IP address
--------	-------	-----------	------------

Parameter	Description
<b>ACL Capability</b>	Enable or disable the ACL function
<b>Enable</b>	Check to enable this ACL entry
<b>Interface</b>	Select the interface domain: LAN or WAN
<b>IP Address</b>	Enter the IP address that is allowed to access the router.
<b>Subnet Mask</b>	Enter the Subnet Mask that is allowed to access the router.
<b>ACL Table</b>	The ACL settings will be listed here. You can click "Delete Selected" to delete the settings you have selected. If you want remove all settings from the table, just click "Delete All" button.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP Address as the DMZ Host, all incoming packets will be checked by the firewall and NAT algorithms then passed to the DMZ Host.

For example, if you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host.

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. The 'Firewall' tab is selected, and the 'DMZ' sub-tab is active. The DMZ section explains that a Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to the local private network. It lists typical DMZ host devices: Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers. Below this, there are radio buttons for 'DMZ Host' settings, with 'Disable' selected and 'Enable' unselected. A text input field for 'DMZ Host IP Address' is present, followed by an 'Apply' button.

Parameter	Description
<b>DMZ Host</b>	Check the item to enable the DMZ function.
<b>DMZ Host IP Address</b>	Enter a static IP Address to the DMZ Host. This IP Address will be exposed to the Internet.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## 14 TOOLBOX Settings

---

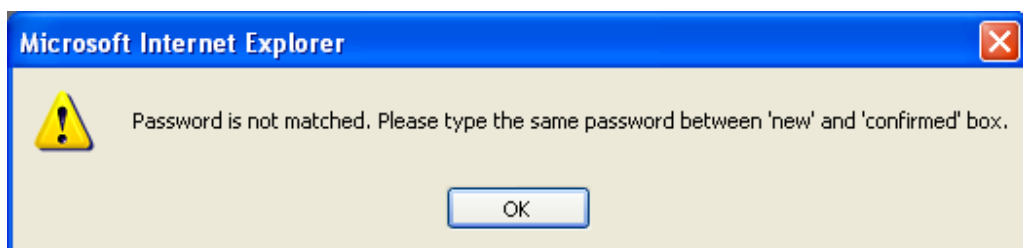
### Password

This page allows you to set the password to access the web server of the router. Please select the "admin (as administrator)" or "user (as user)" account and configure the password.



When you finish, click 'Apply Changes'.

If the password you typed in 'New Password' and 'Confirmed Password' field are not the same, you'll see the following message:



Please retype the new password again when you see above message.

If you see the following message:

**ERROR: Password is not matched !**

OK

It means the content in 'Current Password' field is wrong, please click 'OK' to go back to previous menu, and try to input current password again.

If the current and new passwords are correctly entered, after you click 'Apply', you'll be prompted to input your new password:

A Windows-style dialog box titled "Connect to 192.168.2.1" with a blue header bar containing a question mark and a close button. The main area has a light beige background. At the top left is an icon of two keys. Below it, the text "Default: admin/1234" is displayed. There are two input fields: "User name:" with a dropdown menu showing a user icon, and "Password:" with a standard text box. Below the password field is a checkbox labeled "Remember my password". At the bottom right are "OK" and "Cancel" buttons.

Connect to 192.168.2.1

Default: admin/1234

User name:

Password:

☐ Remember my password

OK Cancel

Please use new password to enter web management interface again, and you should be able to login with new password.

## Time Zone

The Time Zone allows your router to set its time; especially for recording System Log.

wireless  
**modem router** 300N  
SITECOM

Home | Setup Wizard | Basic Settings | Advanced Settings | Firewall | **Toolbox** | Choose your language ▾

Password | **Timezone** | Remote access | Firmware | Back-up | Reset | Diagnostics

### Time Zone Setting

You can maintain the system time by synchronizing with a public time server over the Internet.

**Current Time :** Year 2000 Month 1 Day 1  
Hour 1 Minute 38 Seconds 5

**Time Zone Select :** (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▾

☐ **Enable SNTP client update**

**Time server (NTP) :** ☒ 203.117.180.36 - Asia Pacific ☐ 207.171.3.6 Manual settings

Apply Refresh

Parameter	Description
<b>Current Time</b>	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP server.
<b>Time Zone Select</b>	Select the time zone of the country you are currently in. The router will set its time based on your selection.
<b>Enable SNTP client update</b>	Check the box to enable router to update time from SNTP server.
<b>SNTP server</b>	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings and restart the router so the settings will take effect after it reboots.

## Remote Access

The Remote Access function can secure remote host access to your router from LAN and WAN interfaces for some services provided by the router. These services include Telnet, FTP, TFTP, HTTP, SNMP and PING.

Please click 'System' menu on the left of web management interface, then click 'Remote Management', and the following page will be displayed on your web browser:

wireless  
**modem router** 300N  
SITECOM

Home Setup Wizard Basic Settings Advanced Settings Firewall **Toolbox** Choose your language ▾

Password Timezone **Remote access** Firmware Back-up Reset Diagnostics

**Remote Access**

This page is used to enable/disable management services for the LAN and WAN.

Service Name	LAN	WAN	WAN Port
TELNET	<input checked="" type="checkbox"/>	<input type="checkbox"/>	23
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	21
TFTP	<input type="checkbox"/>	<input type="checkbox"/>	
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	80
SNMP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
PING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Apply

Parameter	Description
LAN	Check/un-check the services on the LAN column to allow/un-allow the services access from LAN side.
WAN	Check/un-check the services on the WAN column to allow/un-allow the services access from WAN side.
WAN Port	This field allows the user to specify the port of the corresponding to the service. Take the HTTP service for example; when it is changed to 8080, the HTTP server address for the WAN side is <a href="http://dsl_addr:8080">http://dsl_addr:8080</a> , where the "dsl addr" is the WAN side IP address of the router.

When you finish, click 'Apply Changes'. You'll see the following message displayed on web browser:



Press 'Continue' to save the settings made and back to web management interface; press 'Apply' to save the settings made and restart the router so the settings will take effect after it reboots.

## Firmware Upgrade

This page allows you to upgrade the firmware for the router. Click "Browse" button to select the firmware file and click "Upload" button to start upgrading.

**IMPORTANT!** Do not turn off your router while this procedure is in progress.

The screenshot shows the web management interface of a Sitecom wireless modem router 300N. The page is titled "wireless modem router 300N" and features the Sitecom logo. A navigation bar at the top includes links for Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. A secondary navigation bar contains tabs for Password, Timezone, Remote access, Firmware (which is the active tab), Back-up, Reset, and Diagnostics. The main content area is titled "Upgrade firmware" and contains a warning: "This page allows you upgrade the ADSL Router firmware to new version. The firmware is the operating software of your router. Please note, do not power off the device during the upload because it may crash the system." Below this, there is a section for "enable automatic firmware update:" with radio buttons for "Enable" and "Disable" (which is selected). A file selection area includes a "Select a File :" label, a text input field, and a "Browse..." button. At the bottom right of the form, there are "Upload" and "Reset" buttons.

## Configuration Tools

This page allows you to backup the current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory defaults.

The screenshot shows the configuration interface for a Sitecom wireless modem router 300N. The page has a header with the product name and a navigation bar with tabs: Home, Setup Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. Below the navigation bar is a sub-menu with tabs: Password, Timezone, Remote access, Firmware, Back-up, Reset, and Diagnostics. The main content area is titled "Backup/Restore Settings" and contains a description: "This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default." Below the description are three sections: "Save Settings to File" with a "Save" button, "Load Settings from File" with a text input field, a "Browse..." button, and an "Upload" button, and "Reset Settings to Default" with a "Reset" button.

Parameter	Description
<b>Save Settings to File</b>	Click Save button to save the ADSL router current configuration to a file named "config.bin" on your PC.
<b>Load Settings from File</b>	Click Browse button to search the file you have saved before and click Upload button to restore the saved configuration to the ADSL router.
<b>Restore Settings to Default</b>	Click Reset button if you want to force the ADSL router to perform a power reset and restore the original factory settings.



## Reboot

Whenever you use the Web configuration to change system settings, the changes are initially placed in temporary storage. To save your change for future use, you have to click "Apply" to reboot the router. If you have encountered problems during the configuration, You can click the "OPS" button in the top panel of the router over 15 seconds to reset default settings.



## Diagnostics

wireless  
**modem router** 300N  
SITECOM

Home Setup Wizard Basic Settings Advanced Settings Firewall **Toolbox** Choose your language ▼

Password Timezone Remote access Firmware Back-up Reset **Diagnostics**

**Diagnostic tools**

This page offers you some diagnostic tools to test your connection. With the ping tool you can check if a remote host is answering. OAM fault management gives you the possibility to check a segment for errors and the diagnostic test is a fully automated connection test.

**Ping tool :**

Host Address :

Ping

**OAM Fault Management :**

Select PVC :

Flow Type : ☒ F5 Segment ☐ F5 End-to-End

Loopback Location ID : FFFFFFFFFFFFFFFFFFFFFFFFFF

Start test

**Diagnostic test :**

Select the Internet Connection : ▼

Start test

### Ping

Once you have your router configured, you can send a ping command to the host you specify in this page. To use it, you must know the IP address of the host you are trying to communicate with and enter the IP address in the Host Address field.

### ATM Loopback

In order to isolate the ATM interface problems, you can use ATM OAM loopback cells to verify connectivity between VP/VC endpoints, as well as segment endpoints within the VP/VC. This page allows you to use ATM ping to test the reachable of a segment endpoint or a connection endpoint.

Parameter	Description
<b>Select PVC</b>	Select the PVC channel you want to do the loop-back diagnostic.
<b>Flow Type</b>	The ATM OAM flow type. The selection can be F5 Segment or F5 End-to-End. ATM uses F4 and F5 cell flows as follows: F4: used in VPs F5: used in VCs
<b>Loopback Location ID</b>	The loop-back location ID field of the loop-back cell. The default value is all 1s (ones) to indicate the endpoint of the segment or connection.

Click "**Start test**" to save the setting to the configuration.

## **Diagnostic Test**

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.